UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,349	08/15/2001	Hiroshi Maruyama	JP920000204US1	3452

7590 10/20/2004	EXAMINER
IBM CORPORATION	DINH, MINH

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
     closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-37* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-37* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *15 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☒ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
        application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-35 and 37-38 have been examined.

Priority

2.   Acknowledgment is made of applicant's claim for foreign priority based on an

application filed in Japan on 08/31/2000. It is noted, however, that applicant has not

filed a certified copy of the 2000-262955 application as required by 35 U.S.C. 119(b).

3.   Should applicant desire to obtain the benefit of foreign priority under 35

U.S.C. 119(a)-(d) prior to declaration of an interference, a translation of the foreign

application should be submitted under 37 CFR 1.55 in reply to this action.

Oath/Declaration

4.   The oath or declaration is defective. A new oath or declaration in compliance

with 37 CFR 1.67(a) identifying this application by application number and filing date is

required. See MPEP §§ 602.01 and 602.02.

> The oath or declaration is defective because:
> The full name of the first inventor (family name and at least one given name
> together with any initial) has not been set forth in the Declaration filed 1/8/2002.

Claim Objections

5.   The numbering of claims is objected to because the claims are not numbered

consecutively (claims 1-35 and 37-38). Misnumbered claims 37 and 38 have been

renumbered 36 and 37 respectively.

Claim Rejections - 35 USC § 112

6.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

7.   Claims 7-12, 14, 17-21 and 25 are rejected under 35 U.S.C. 112, second

paragraph, as being indefinite for failing to particularly point out and distinctly claim the

subject matter which applicant regards as the invention.

a.   Regarding claims 7-12, 14 and 17-21, it is not clear where the corresponding

structure for the means plus function to be found in the specification.

b.   Regarding claim 25, it recites the limitation "said summary text" in the 5th-6th

lines. There is insufficient antecedent basis for this limitation in the claim. The limitation

is interpreted as "a summary text".

Claim Rejections - 35 USC § 102

8.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public
> use or on sale in this country, more than one year prior to the date of application for patent in the United
> States.

9.   Claims 1, 6-7, 12, 19, 22, 25-26, 29, 32 and 35-37 are rejected under 35

U.S.C. 102(b) as being anticipated by the reference "WMLScript Crypto Library".

a.   Regarding claims 1, 6-7, 12, 25-26, 29 and 32, "WMLScript Crypto Library"

discloses a method comprising:

generating summary text for an electronic document (Section 5.1.1 Introduction,

"Many kind of application ... other financial document"; p. 10, Example);

displaying said summary text on the display screen of a terminal of a signatory

(Section 5.1.1, Introduction, "To support this requirement ... accountabilities purpose");

calculating a digest value for said summary text using a hash function (Appendix

B. RSA PKCS#1 Signature Calculation);

encrypting data, including said digest value, using a private key stored in said

terminal, and generating a signature value (Section 5.1.1, Introduction, "The browser

SHOULD ... signature computation"); and

generating a signed document including said signature value (Section 5.1.1,

Introduction, "To support this requirement ... accountabilities purpose").

b.   Regarding claims 19, 22 and 35-37, "WMLScript Crypto Library", in addition to

the limitations in claim 1, further discloses receiving summary text for an electronic

document (Section 6.1 Usage with signText).

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

11.   Claims 2 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over

"WMLScript Crypto Library" as applied to claims 1 and 7 above, and further in view of

Rys et al. (6,704,736). "WMLScript Crypto Library" does not disclose using XML and an

Xpath parser. Rys discloses using XML (col. 1, lines 36-47) and an Xpath parser (col.

6, lines 16-34). It would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify the method in "WMLScript Crypto Library" to use XML

and an Xpath parser, as taught by Rys. XML is a tag-oriented language, and tags

permit the creator of the data to express the semantics of the data and to capture the

hierarchical relationships in the data in a way that is self-describing. An Xpath parser is

capable of identifying nodes in hierarchical data.

12.   Claims 3 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

"WMLScript Crypto Library" as applied to claims 1, 7 above, and further in view of

Berringer et al. (US 2004/0181756 A1). "WMLScript Crypto Library" does not disclose

using a signature template having a variable field for said digest value, employing said

function to convert said signature template to which said digest value has been added,

and employing said private key to encrypt a value obtained by conversion and

generating said signature value. Berringer disclose a method for generating an

electronic document with embedded digital signature using a signature template, the

method comprising the steps of using a signature template having a variable field for

said digest value, employing a function to convert said signature template to which said

digest value has been added, and employing a private key to encrypt a value obtained by conversion and generating said signature value (paragraphs 0011-0013). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method in "WMLScript Crypto Library" to use a signature template, as taught by Berringer. A template having a predefined format can be used for many documents.

13. Claims 4-5 and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over "WMLScript Crypto Library" in view of Berringer as applied to claim 3 above, and further in view of "XML-Signature Core Syntax". "WMLScript Crypto Library" and Berringer do not disclose that a URI for the electronic document is part of the data to be signed and using a canonicalization algorithm. "XML-Signature Core Syntax" discloses a method for generating XML signatures. Specifically, the reference discloses that the URI of an electronic document is part of the data to be signed and a canonicalization algorithm is used in the process (Section 8.1 Generation). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the method in the "XML-Signature Core Syntax" reference into the combined method of "WMLScript Crypto Library" and Berringer, so that digital signatures could be applied to XML documents and other Internet resources (Section 1.0 Introduction).

14.   Claims 13-15, 17, 27-28, 30-31 and 33-34 are rejected under 35 U.S.C. 103(a)

as being unpatentable over "WMLScript Crypto Library" in view of Brown et al.

(6,671,805). The "WMLScript Crypto Library" reference discloses a method comprising:

a signature demandant generating summary text for an electronic document, and

transmitting said summary text to a terminal of a signatory (Section 5.1.1 Introduction,

"Many kind of application ... other financial document"; p. 10, Example; Section 6.1

Usage with signText);

said signatory displaying said summary text on the display screen of said

terminal of said signatory (Section 5.1.1, Introduction, "To support this requirement ...

accountabilities purpose");

said signatory confirming said summary text, and employing a private key stored

in said terminal to digitally sign said summary text or a document corresponding to said

summary text (Section 5.1.1, Introduction, ""The browser SHOULD ... signature

computation");

said signatory generating a signed document by adding said signature value to

said electronic document (Section 5.1.1, Introduction, "To support this requirement ...

accountabilities purpose"); and

said signatory transmitting said signed document to said signature demandant

(Section 5.1.1 Introduction, "Many kind of application ... other financial document";

Section 6.1 Usage with signText).

"WMLScript Crypto Library" does not disclose utilizing an agent to generate

summary text for the electronic document and generate the signed document. Brown

discloses a digital signature method utilizing an agent to generate summary text for an electronic document (col. 18, line 55 – col. 19, line 9). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify "WMLScript Crypto Library" method to utilize an agent to generate summary text for the electronic document, as taught by Brown, in order to save time and effort while increasing accuracy (col. 18, lines 63-65). Accordingly, the agent receives a signature value from the signatory and generates the signed document.

15.   Claims 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over "WMLScript Crypto Library" in view of Brown as applied to claims 15 and 17 above, and further in view of Rys. "WMLScript Crypto Library" does not disclose using XML and an Xpath parser. Rys discloses using XML (col. 1, lines 36-47) and an Xpath parser (col. 6, lines 16-34). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of "WMLScript Crypto Library" and Brown to use XML and an Xpath parser, as taught by Rys. XML is a tag-oriented language, and tags permit the creator of the data to express the semantics of the data and to capture the hierarchical relationships in the data in a way that is self-describing. An Xpath parser is capable of identifying nodes in hierarchical data.

16.   Claims 20-21 and 23-24 are rejected under 35 U.S.C. 103(a) as being

unpatentable over "WMLScript Crypto Library" as applied to claims 19 and 22 above,

and further in view of Berringer and "XML-Signature Core Syntax".

"WMLScript Crypto Library" does not disclose using a signature template having

a variable field for said digest value, employing said function to convert said signature

template to which said digest value has been added, and employing said private key to

encrypt a value obtained by conversion and generating said signature value. Berringer

disclose a method for generating an electronic document with embedded digital

signature using a signature template, the method comprising the steps of using a

signature template having a variable field for said digest value, employing a function to

convert said signature template to which said digest value has been added, and

employing a private key to encrypt a value obtained by conversion and generating said

signature value (paragraphs 0011-0013). It would have been obvious to one of ordinary

skill in the art at the time the invention was made to modify the method in "WMLScript

Crypto Library" to use a signature template, as taught by Berringer. A template having

a predefined format can be used for many documents.

"WMLScript Crypto Library" does not disclose that a URI for the electronic

document is part of the data to be signed and using a canonicalization algorithm. "XML-

Signature Core Syntax" discloses a method for generating XML signatures.

Specifically, the reference discloses that the URI of an electronic document is part of the

data to be signed and a canonicalization algorithm is used in the process (Section 8.1

Generation). It would have been obvious to one of ordinary skill in the art at the time

the invention was made to incorporate the method in the "XML-Signature Core Syntax"

reference into the method of "WMLScript Crypto Library", so that digital signatures could

be applied to XML documents and other Internet resources (Section 1.0 Introduction).

Conclusion

17.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

        Capers et al. (US 2002/0112009 A1) discloses a method for providing data

applications for a mobile device.

        Cseri et al. (US 2003/0046317 A1) discloses a method for providing an XML

binary format.

        Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Minh Dinh whose telephone number is 703-306-5617.

The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

10/15/04

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100